CLAIMS

We claim:

1. A method comprising:

a) providing with a source ATM at least one table of data;

b) generating with the source ATM a hard key responsive to the at least one table of data;

c) generating with the source ATM a data file that includes random information;

d) generating with the source ATM a factory key responsive to the at least one table of data and responsive to at least one first portion of the random information;

e) encrypting with the source ATM at least one secret encryption key responsive to the factory key;

f) including the encrypted at least one secret encryption key in the data file;

g) encrypting with the source ATM the data file using the hard key; and

h) storing the encrypted data file on at least one portable storage medium in operative connection with the source ATM.

2. The method according to claim 1 further comprising:

i) receiving the at least one secret encryption key through at least one input device of the source ATM.

3. The method according to claim 2, wherein the at least one input device includes a keypad.

4. The method according to claim 2, wherein the source ATM includes at least one first terminal control software component that is operative to cause a computer in the source ATM to carry out steps (a) through (h), wherein the at least one first terminal control software component includes at least a first portion of the at least one table of data embedded therein.

5. The method according to claim 4, wherein the source ATM includes at least one hardware device, wherein the at least one hardware device includes at least a second portion of the at least one table of data stored therein.

6. The method according to claim 5, wherein the at least one hardware device includes an encrypting pin pad.

7. The method according to claim 4, wherein the at least one portable storage medium includes a floppy disk.

8. The method according to claim 4, wherein further comprising:

j) generating with the source ATM at least one first seed value;

k) modifying with the source ATM the at least one first seed value, responsive to at least one input received through operation of at least one input device of the source ATM; and

wherein in step (c) the random information is generated by the source ATM responsive to the at least one first seed value.

9. The method according to claim 8, wherein prior to step (c) further comprising:

l) determining a time value that corresponds to about when the at least one first terminal control software component is started in at least one computer of the ATM;

m) generating with the source ATM at least one second seed value responsive to the time value; and

wherein in step (c) the random information is further generated by the source ATM responsive to the at least one second seed value.

10. The method according to claim 1, wherein prior to step (g) further comprising:

i) padding the data file with at least one second portion of the random information.

11. The method according to claim 10, wherein in step (h) the encrypted file has a size which corresponds to about the maximum storage capacity of the at least one portable storage medium.

12. The method according to claim 1, wherein the factory key and the hard key correspond to DES keys, wherein in steps (e) and (g) encrypting of the at least one secret encryption key and the data file is performed using a DES encryption algorithm.

13. The method according to claim 1, wherein prior to step (g) further comprising:

i) generating at least one first message authentication check (MAC) value responsive to the at least one secret encryption key; and

j) including the at least one first MAC value in the file.

14. The method according to claim 1, wherein the factory key is comprised of a left portion and a right portion, wherein step (d) includes:

i) generating a first block of data using the at least one table of data and the at least one first portion of the random information;

j) generating a first message authentication check (MAC) for the first block of data, wherein the first MAC value corresponds to the left portion of the factory key;

k) generating a second block of data using the at least one table of data and the at least one first portion of the random information; and

l) generating a second MAC value for the second block of data, wherein the second MAC value corresponds to the right portion of the factory key, wherein the second MAC value is different than the first MAC value.

15. The method according to claim 14, further comprising:

m) selecting a first subset of the first block of data, wherein in step (j) the first MAC value is generated using the first subset of the first block of data as a key;

n) selecting a second subset of the second block of data wherein in step (l) the second MAC value is generated using the second subset of the second block of data as a key.

16. The method according to claim 15, wherein prior to step (i) further comprising:

o) determining at least one offset value, wherein in steps (m) and (n) the first and second subsets of the corresponding first and second blocks of data are selected responsive to the at least one offset value.

17. The method according to claim 14, wherein prior to step (g) further comprising:

m) generating at least one third MAC value for at least the at least one secret encryption key using at least one of the left portion or the right portion of the factory key;

n) including the at least one third MAC value in the file.

18. The method according to claim 14, wherein step (i) includes concatenating bytes from the at least one table of data and the at least one first portion of the random information in a first order, wherein step (k) includes concatenating bytes from the at least one table of data and the at least one first portion of the random information in a second order that is different than the first order.

19. The method according to claim 18, wherein in step (i) the first order includes an alternating progression of the bytes from the at least one table of data and the at least one first portion of the random information, wherein in step (k) the second order includes an opposite alternating progression of the bytes from the at least one table of data and the at least one first portion of the random information.

20. The method according to claim 1, wherein the hard key is comprised of a left portion and a right portion, wherein step (b) includes:

i) generating a first block of data using the at least one table of data;

j) generating a first message authentication check (MAC) value for the first block of data, wherein the first MAC value corresponds to the left portion of the hard key.

k) generating a second block of data using the at least one table of data; and

l) generating a second MAC value for the second block of, wherein the second MAC value corresponds to the right portion of the hard key, wherein the second MAC value is different than the first MAC value.

21. The method according to claim 19, wherein further comprising:

m) selecting a first subset of the first block of data, wherein in step (j) the first MAC value is generated using the first subset of the first block of data as a key

n) selecting a second subset of the second block of data, wherein in step (j) the second MAC value is generated data using the second subset of the second block of data as a key.

22. The method according to claim 1, wherein the source ATM includes a cash dispenser, wherein further comprising:

i) dispensing cash with the cash dispenser.

23. The method according to claim 1 comprising:

i) providing with a target ATM the at least one table of data;

j) generating with the target ATM the hard key responsive to the at least one table of data;

k) accessing with the target ATM the data file from the at least one portable storage medium;

l) decrypting with the target ATM the data file using the hard key;

m) accessing with the target ATM the at least one first portion of the random information from the decrypted data file;

n) accessing with the target ATM the at least one encrypted secret encryption key from the decrypted data file;

o) generating with the target ATM the factory key responsive to the at least one table of data and responsive to the at least one first portion of the random information;

p) decrypting with the target ATM the at least one encrypted secret encryption key responsive to the factory key to produce the at least one secret encryption key.

24. The method according to claim 23, wherein the target ATM includes a cash dispenser, wherein further comprising:

q) configuring the target ATM responsive to the at least one secret encryption key, wherein the target ATM is enabled to dispense cash using the cash dispenser; and

r) dispensing cash with the cash dispenser.

25. The method according to claim 24, wherein the target ATM includes at least one second terminal control software component that is operative to cause a computer in the target ATM to carry out steps (i) through (p), wherein the at least one second terminal control software component includes at least the first portion of the at least one table of data embedded therein.

26. The method according to claim 25, wherein the target ATM includes at least one hardware device, wherein the at least one hardware device of the target ATM includes at least the second portion of the at least one table of data stored therein.

27. The method according to claim 26, wherein the at least one hardware device of the target ATM includes an encrypting pin pad.

28. The method according to claim 23, further comprising:

q) accessing with the target ATM the at least one first message authentication check (MAC) value from the decrypted file;

r) generating with the target ATM at least one second MAC value responsive to the at least one secret encryption key; and

s) verifying with the target ATM that the at least one first MAC value corresponds to the at least one second MAC value.

29. The method according to claim 23, wherein prior to step (g) further comprising:

i) including an expiration date in the data file;

wherein further comprising;

j) accessing with the target ATM, the expiration date from the data file;

k) determining a current date with the target ATM; and

l) verifying with the target ATM that the expiration date does not exceed the current date.

30. A method comprising:

a) providing with a target ATM at least one table of data;

b) generating with the target ATM a hard key responsive to the at least one table of data;

c) accessing with the target ATM a data file from at least one portable storage medium;

d) decrypting with the target ATM the data file using the hard key;

e) accessing with the target ATM at least one seed key data from the decrypted data file;

f) accessing with the target ATM at least one encrypted secret encryption key from the decrypted data file;

g) generating with the target ATM a factory key responsive to the at least one table of data and responsive to the at least one seed key data;

h) decrypting with the target ATM the at least one encrypted secret encryption key responsive to the factory key to produce the at least one secret encryption key.

31. The method according to claim 30, wherein the target ATM includes a cash dispenser, wherein further comprising:

i) configuring the target ATM responsive to the at least one secret encryption key, wherein the target ATM is enabled to dispense cash using the cash dispenser; and

j) dispensing cash with the cash dispenser.

32. The method according to claim 31, wherein the at least one secret encryption key corresponds to a terminal master key, wherein step (i) includes:

k) receiving with the target ATM at least one encrypted communication key from a host system;

l) decrypting with the target ATM the encrypted communication key using the terminal master key to produce the communication key, wherein the target ATM is operative to securely send a personal identification number (PIN) inputted through at least one input device of the target ATM to the host system using the communication key.

33. The method according to claim 31, wherein the target ATM includes at least one first terminal control software component that is operative to cause a computer in the target ATM to

carry out steps (a) through (h), wherein the at least one first terminal control software component includes at least a first portion of the at least one table of data embedded therein.

34. The method according to claim 33, wherein the target ATM includes at least one hardware device, wherein the at least one hardware device includes at least a second portion of the at least one table of data stored therein.

35. The method according to claim 34, wherein the at least one hardware device includes an encrypting pin pad.

36. The method according to claim 30, further comprising:

i) accessing with the target ATM at least one first message authentication check (MAC) value from the decrypted file;

j) generating with the target ATM at least one second MAC value responsive to the at least one secret encryption key; and

k) verifying with the target ATM that the at least one first MAC value corresponds to the at least one second MAC value.

37. The method according to claim 30, wherein the factory key is comprised of a left portion and a right portion, wherein step (g) includes:

i) generating a first block of data using the at least one table of data and the at least one seed key data;

j) generating a first message authentication check (MAC) value for the first block of data, wherein the first MAC value corresponds to the left portion of the factory key;

k) generating a second block of data using the at least one table of data and the at least one first portion of the decrypted file; and

l) generating a second MAC value for the second block of data, wherein the second MAC value corresponds to the right portion of the factory key, wherein the second MAC value is different than the first MAC value.

38. The method according to claim 37, further comprising:

m) selecting a first subset of the first block of data, wherein the first MAC value is generated using the first subset of the first block of data as a key;

n) selecting a second subset of the second block of data, wherein the second MAC value is generated using the second subset of the second block of data as a key.

39. The method according to claim 38, wherein prior to step (i) further comprising:

o) determining at least one offset value, wherein in steps (m) and (n) the first and second subsets of the corresponding first and second blocks of data are selected responsive to the at least one offset value.

40. The method according to claim 37, wherein prior to step (g) further comprising:

m) accessing with the target ATM at least one third MAC value from the decrypted file;

n) generating with the target ATM at least one fourth MAC value for at least the at least one secret encryption key using at least one of the left portion or the right portion of the factory key; and

o) verifying with the target ATM that the at least one third MAC value corresponds to the at least one fourth MAC value.

41. The method according to claim 31, wherein step (i) includes concatenating bytes from the at least one table of data and the at least one seed key data in a first order, wherein step (k) includes concatenating bytes from the at least one table of data and the at least one seed key data in a second order that is different than the first order.

42. The method according to claim 41, wherein in step (i) the first order includes an alternating progression of the bytes from the at least one table of data and the at least one seed key data, wherein in step (k) the second order includes an opposite alternating progression of the bytes from the at least one table of data and the at least one seed key data.

43. The method according to claim 30, wherein the hard key is comprised of a left portion and a right portion, wherein step (b) includes:

i) generating a first block of data using the at least one table of data;

j) generating a first message authentication check (MAC) value for the first block of data, wherein the first MAC value corresponds to the left portion of the hard key.

k) generating a second block of data using the at least one table of data; and

l) generating a second MAC value for the second block of data, wherein the second MAC value corresponds to the right portion of the hard key, wherein the second MAC value is different than the first MAC value.

44. The method according to claim 43, further comprising

m) selecting a first subset of the first block of data, wherein in step (j) the first MAC value is generated using the first subset of the first block of data as a key;

n) selecting a second subset of the second block of data, wherein in step (k) the second MAC value is generated using the second subset of the second block of data as a key.

45. The method according to claim 30, wherein the data file includes an expiration date, wherein further comprising:

i) accessing with the target ATM the expiration date from the data file ;

j) determining a current date with the target ATM; and

k) verifying with the target ATM that the expiration date does not exceed the current date.

46. The method according to claim 30, wherein the at least one portable storage medium includes a floppy disk.

47. The method according to claim 30, wherein the factory key and the hard key correspond to DES keys, wherein in steps (e) and (g) encrypting of the at least one secret encryption key and the data file is performed using a DES encryption algorithm.